Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	SERVER-MAIL Phishing attempt possible download of malware	High	The user opened a phishing email sent to hr@inergy.com and clicked on a malicious attachment or link. Suspicious indicators: - Sender domain: 76tguyhh6tgftrt7tg.su (unusual format) - Sender IP address: 114.114.114.114 The incident involves possible malware delivery via phishing.	Escalated

Ticket comments
Phishing email identified from <76tguyhh6tgftrt7tg.su> with malicious attachment "bfsvc.exe". The file hash matched known malware (SHA-256: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b). VirusTotal confirmed this malware is malicious. This incident matches fishing behavior with password-protected file and fake job application . Recommend : - blocking sender domain and IP. - isolating affected host - notify the receiver employee - running a full antivirus scan.

Additional indicators: suspicious domain name and grammar errors in the email body.

5 W's of the Phishing Incident

- Who caused the incident?
  The attacker using the email address 76tguyhh6tgftrt7tg.su with IP address 114.114.114.114.

- What happened?
  A phishing email pretending to be a job application was sent with a malicious, password-protected attachment (bfsvc.exe). The file hash was verified as malware by VirusTotal.

- When did the incident take place?
  Wednesday, July 20, 2022, at 09:30:14 AM.

- Where did the incident occur?
  On the recipient's device at the organization (email: hr@inergy.com).

- Why did it happen?
  The attacker used social engineering (fake job application and resume) to trick the recipient into opening a malicious file and compromise the system.

Reasons the phishing alert is legitimate:

1. The file hash matched known malware (confirmed by VirusTotal).
2. The sender's domain and IP are suspicious and do not belong to a known business.
3. The email follows a known phishing pattern: fake job application, password-protected file, grammar errors.

Additional information

Known malicious file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email:
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>
Sent: Wednesday, July 20, 2022 09:30:14 AM
To: <hr@inergy.com> <176.157.125.93>
Subject: Re: Infrastructure Egnieer role

Dear HR at Ingergy,

I am writing for to express my interest in the engineer role posted from the website.

There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,

Clyde West
Attachment: filename="bfsvc.exe"